

DORSEY & WHITNEY LLP

File No. A-71400/DJB/MAK

Applicant(s): Timothy Winston HIBBERD
Serial No.: 10/088,034
For: **An Access Control Method**

JK

Please acknowledge receipt of the enclosed:

1. Transmittal of Missing Requirements.
2. Copy of the Notification of Missing Requirements Under 35 U.S.C. 371, etc.
3. Petition for Extension of Time (1 mo.)
4. Check No. 1554 in the amount of \$110.00
5. Declaration for Patent Application
6. Assignment with Form PTO-1595
7. Check No. 1553 in the amount of \$40.00
8. Power of Attorney by Assignee

by imprinting the Patent Office "date stamp" hereon and returning to the addressee indicated on the reverse.

Due date: 29 July 2002 extended to 29 August 2002

Date of mailing: 20 August 2002

SF-1090725v1

DT06 Rec'd PCT/PTO 26 AUG 2002

[461124-00038]



DORSEY & WHITNEY LLP

File No. A-71400/DJB/MAK

Applicant(s): Timothy Winston HIBBERD
Serial No.: 10/088,034
For: **An Access Control Method**

Please acknowledge receipt of the enclosed:

1. Transmittal of Missing Requirements.
 2. Copy of the Notification of Missing Requirements Under 35 U.S.C. 371, etc.
 3. Petition for Extension of Time (1 mo.)
 4. Check No. 1554 in the amount of \$110.00
 5. Declaration for Patent Application
 6. Assignment with Form PTO-1595
 7. Check No. 1553 in the amount of \$40.00
 8. Power of Attorney by Assignee
- by imprinting the Patent Office "date stamp" hereon and returning to the addressee indicated on the reverse.

Due date: 29 July 2002 extended to 29 August 2002

Date of mailing: 20 August 2002

SF-1090725v1

[461124-00038]

PATENT

Attorney Docket No.: A-71400/DJB/MAK

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

<u>In re</u> application of:)	Examiner:	Not Yet Known
)		
Timothy Winston HIBBERD)	Group Art Unit:	Not Yet Known
)		
Serial No.: 10/088,034)		
)		
Filing Date: 12 March 2002)		
)		
For: <i>An Access Control Method</i>)		
_____)		

CERTIFICATE OF MAILING

I hereby certify that this correspondence, including listed enclosures, is being deposited with the United States Postal Service, as First Class Mail in an envelope addressed to: Box PCT, Assistant Commissioner for Patents, Washington, DC 20231 on 20 August 2002.

Signed: _____

Todd V. LEONE

TRANSMITTAL OF MISSING REQUIREMENTS
AND REQUEST FOR CORRECTED FILING RECEIPT

Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

This transmittal is in response to the Notification of Missing Requirements Under 35 U.S.C. 371 in the United States Designated/Elected Office (DO/EO/US) mailed 29 May 2002.

Applicants submit the following items:

1. This Transmittal of Missing Requirements.
2. A copy of the Notification of Missing Requirements Under 35 U.S.C. 371 in the United States Designated/Elected Office (DO/EO/US) as referenced hereinabove.
3. Petition for Extension of Time (1 month.)

4. Our Check No. 1554 in the amount of \$110.00 to pay the extension fee.
5. Declaration for Patent Application.
6. Assignment with Form PTO-1595 Recordation Form Cover Sheet.
7. Our Check No. 1553 in the amount of \$40.00 to pay the recordation fee.
8. Power of Attorney by Assignee.

Applicant notes that the inventor's name as it appears on the Notification of Missing Requirements is incorrect as it appears. Please correct the name to read "Timothy Winston HIBBERD" (rather than "timothy Winston").

The Commissioner is hereby authorized to charge any additional fees that may be required, including extension fees, or credit any overpayment to Deposit Account No. 50-2319 (our Order No. 461124-00038 [A-71400]).

Date: 20 August 2002

Respectfully submitted,

DORSEY & WHITNEY LLP

By: Michael A. Kaufman
Michael A. KAUFMAN

Reg. No. 32,998

Filed under 37 C.F.R. § 1.34(a)

Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187
Telephone: (415) 781-1989
Facsimile: (415) 398-3249



UNITED STATES PATENT AND TRADEMARK OFFICE

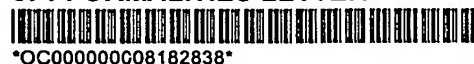
Commissioner for Patents, Box PCT
United States Patent and Trademark Office
Washington, D.C. 20231
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
10/088,034	timothy Winston	A-71400-DJB/MAK

Michael A Kaufman
Flehr Hohbach Test
Albritton & Herbert
Four Embarcadero Center suite 3400
San Fransisco, CA 94111-4187

INTERNATIONAL APPLICATION NO.	
PCT/AU00/01095	
I.A. FILING DATE	PRIORITY DATE
09/13/2000	09/13/1999

CONFIRMATION NO. 6572
371 FORMALITIES LETTER



Date Mailed: 05/29/2002

NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as an Elected Office (37 CFR 1.495):

- U.S. Basic National Fees
- Priority Document
- Copy of IPE Report
- Copy of the International Application
- Copy of the International Search Report
- Preliminary Amendments
- Request for Immediate Examination

File A-71400 Atty DJB/MAK
Due Date 7/29/2002
Type Missg P/B Refs

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date.

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTH FROM THE DATE OF THIS NOTICE OR BY 22 or 32 MONTHS (where 37 CFR 1.495 applies) FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

*A copy of this notice **MUST** be returned with the response.*

INDIA L EVANS

Telephone: (703) 305-2936

PART 1 - ATTORNEY/APPLICANT COPY

U.S. APPLICATION NUMBER NO.	INTERNATIONAL APPLICATION NO.	ATTY. DOCKET NO.
10/088,034	PCT/AU00/01095	A-71400-DJB/MAK

FORM PCT/DO/EO/905 (371 Formalities Notice)

1554

DORSEY & WHITNEY LLP
4 EMBARCADERO CENTER SUITE 3400
SAN FRANCISCO, CA 94111-4187

2-3/710

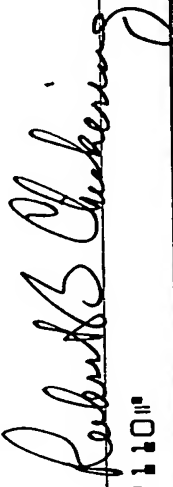
DATE 8/20/2002

PAY TO THE ORDER OF COMMISSIONER OF PATENTS \$ 110.00

ONE HUNDRED AND TEN DOLLARS 1 DOLLARS 

Bank of America.

Commercial Disbursement Account • Chicago, Illinois

Robert S. Chakerian  MP

FOR 115 020048-00006

⑈001554⑈ ⑆⑈071000039⑈ 86660⑈ 17110⑈

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Timothy Winston HIBBERD

File No.: A-71400/DJB/MAK

Serial No.: 10/088,034

Examiner: Not Yet Known

Filing Date: 12 March 2002

Group Art Unit: Not Yet Known

For: **An Access Control Method**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on 20 August 2002.

Signed: _____

Todd V. LEONE

PETITION FOR EXTENSION OF TIME

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Pursuant to 37 C.F.R. 1.136(a), an extension of time of:

	<u>Large Entity</u>		<u>Small Entity</u>	
One Month:	<input checked="" type="checkbox"/>	\$ 110.00	<input type="checkbox"/>	\$ 55.00
Two Months:	<input type="checkbox"/>	\$ 400.00	<input type="checkbox"/>	\$ 200.00
Three Months:	<input type="checkbox"/>	\$ 920.00	<input type="checkbox"/>	\$ 460.00
Four Months:	<input type="checkbox"/>	\$ 1,440.00	<input type="checkbox"/>	\$ 720.00
Five Months:	<input type="checkbox"/>	\$ 1,960.00	<input type="checkbox"/>	\$ 980.00

is hereby requested to

- ☐ respond to the Official Action mailed _____.
- ☐ file a Notice of Appeal in response to a final rejection mailed _____.
- ☐ file an Appeal Brief now due _____.
- ☒ other (specify): respond to the Notice of Missing Requirements Under
35 U.S.C. 371 in the United States Designated/Elected Office
(DO/EO/US) mailed 29 May 2002

The requisite fee pursuant to 37 C.F.R. 1.17 is:

- ☒ enclosed by Check No. 1554.
- ☐ to be charged to Deposit Account No. 50-2319 (Order No. _____).
A duplicate copy of this sheet is enclosed.
- ☒ Please charge any additional fees or credit any overpayment to Deposit Account No. 50-2319 (Order No. 461124-00038 [A-71400]).

Respectfully submitted,

DORSEY & WHITNEY LLP

Date: 20 August 2002

By _____

Michael A. KAUFMAN

Reg. No. 32,998

Filed under 37 C.F.R. § 1.34(a)

Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187
Tel.: (415) 781-1989

DECLARATION FOR PATENT APPLICATION

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled * An access control method

the specification of which

☐ is attached hereto

(Check
one)

☐ was filed on _____ as
Application Serial No. _____
and was amended on _____
(if applicable)

[x] International Patent Application No. PCT/AU00/01095 filed 13 September 2000

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Patent Office all information known to me to be material to patentability as defined in 37 C.F.R. 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
<u>PQ2787/99</u>	<u>Australia</u>	<u>13 September 1999</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
<u>PCT/AU00/01095</u>	<u>PCT</u>	<u>13 September 2000</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
_____	_____	_____	<input type="checkbox"/>	<input type="checkbox"/>
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the Patent Office all information known to me to be material to patentability as defined in 37 C.F.R. 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)
_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)
_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status) (patented, pending, abandoned)

Direct all telephone calls to Michael A. Kaufman at (415) 781-1989.
Address all correspondence to:

FLEHR HOHBACH TEST
ALBRITTON & HERBERT LLP
Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187

File No. _____ *

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor:	* Timothy Winston HIBBERD
Inventor's signature:	<i>Timothy Hibberd</i>
Date:	July 14, 2002
Residence:	* 2/7 Bogota Avenue, Neutral Bay, New South Wales 2089, Australia
Citizenship:	* Canadian
Post Office Address:	* " as above "

Full name of second joint inventor, if any:	*
Inventor's signature:	
Date:	
Residence:	*
Citizenship:	*
Post Office Address:	*

Full name of third joint inventor, if any:	*
Inventor's signature:	
Date:	
Residence:	*
Citizenship:	*
Post Office Address:	*

Full name of fourth joint inventor, if any:	*
Inventor's signature:	
Date:	
Residence:	*
Citizenship:	*

AN ACCESS CONTROL METHOD

The present invention relates to an access control method and to a system and a computer program for executing the method.

5

One of the perennial problems with providing services over a communications network, such as the Internet, is the vulnerability of the system providing the service to damage or attack by malicious parties, such as computer hackers. Particularly for service provision over the Internet, services, such as information provision and communication
10 services, may be accessed using scripts or applets which the hackers can attempt to replicate in programs to execute excessive access requests for the service. The excessive access requests, depending on their nature, can have a variety of effects on the service and in some circumstances may cause the service system to collapse.

15 Detecting a spurious access request or "hack" by a hacker is problematic for any service provider and a considerable number of security procedures have been developed to try and protect systems from a hack. Hackers however have proven particularly adept at being able to circumvent all forms of security procedures and systems which seek to deny them access. Given the computing resources and skills which the hacking community
20 possess, an alternative approach to protecting service provision systems is needed.

In accordance with the present invention there is provided an access control method, including:

- receiving an initial access request for a service from a data processing apparatus;
- 25 sending unique identification data to said apparatus in response to said initial access request; and
- applying a rate limit for verifying access to said service until said identification data is verified by a user of said apparatus.

- 2 -

The present invention also provides an access control method executed by a computer system, including:

- applying an access rate limit until a user issuing access requests is verified;
- a first control level involving verifying said user;
- 5 a second control level applying hack program detection tests to said access requests and verifying said user;
- a third control level requiring use of predetermined download software for transmitting said access requests and verifying said user;
- a fourth control level blocking access to said service on the basis of at least one
- 10 communications address corresponding to said access requests; and
- invoking said control levels sequentially depending on a number of failed attempts to verify said user.

The present invention also provides an access control system having components

15 for executing the steps of the method.

The present invention also provides an access control software stored on a computer system, having code for executing the steps of the access control method

20 The present invention also provides an access control system, including:

- an access control server for receiving access requests for a service from a data processing apparatus, rate limiting access to the server until a user of said apparatus is verified, and sending to said data processing apparatus unique identification data; and
- an IVR for contacting a device having an association with said data processing
- 25 apparatus, issuing a request for said identification data, and providing the data received in response to said request to said access server in order to verify said user.

A preferred embodiment of the present invention is hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

30 Figure 1 is a block diagram of a preferred embodiment of an access control system connected to a communications network.

- 3 -

An access control system 2, as shown in Figure 1, is used to limit access to and protect a service provision system 4. The access control system 2 includes an access control server 6 and an interactive voice response system (IVR) 8 which are both
5 connected to a communications network 30 and to each other. The service system 4 includes a network server 10 connected to the access server 6, and an application server 12 connected to the network server 10 and having access to a database 14. The application server 12 executes the application to provide a service over the network 30 using the data contained in the database 14. The application server 12 gains access to the network 30 via
10 the network server 10, which may be a web server to handle communications with the network using HTTP. The access server 6 is also able to communicate with the network 30 using HTTP and other protocols as necessary. The network 30 includes the Internet and other data and voice delivery networks, such as a public switched telephone network (PSTN). Although the servers 6, 10 and 12 and the IVR 8 are shown as separate machines,
15 the machines can be integrated into one machine or divided into different machines which may be distributed and communicate remotely, as will be understood by those skilled in the art. The latter involves distributing the software components of the servers 6, 10 and 12 and the IVR 8 amongst the different machines.

20 The preferred embodiment is described below with reference to the provision of a service for executing icon calling, where the application server 12 allows parties (an A party) using a data processing apparatus 22 (i.e. a computer) to access directory or telephone information concerning another party (the B party) via a web site, and then select a call icon on a page of the site to establish a call between the A and B parties. This
25 involves the application server 12 instructing the network 30 to place a call to a telephone 16 of the A party and a telephone 18 or 20 of the B party. Further details concerning the system required to support the service is provided in the applicant's Australian Patent Application No. 19173/97. It will of course be apparent to a skilled addressee that the access control method executed by the system 2 described below can be applied to any
30 service delivered over the communications network 30.

- 4 -

The access control method is executed by a computer program stored on the access control server 6 which communicates with and uses the standard features of the IVR 8, such as those provided with the IVRs produced by Periphonics Corporation or Dialogic Corporation. Again, the program could be distributed or its processes executed by
5 dedicated hardware, such as application specific integrated circuits (ASICs), as will be understood by those skilled in the art.

The access control method adopts a different approach to standard security methods, in that it is assumed that a hacker using the apparatus 22 will eventually be able
10 to penetrate any defences, and therefore allows legitimate users to use the system 4 whilst it is under attack. The method seeks to limit the number of access requests for the service that a hacker can make whilst moving through different control levels as the number of access attempts increase over monitored periods of time. For the icon calling service this means limiting the number of prank calls to the same as that which could be made from a
15 telephone. In other words, this involves rate limiting the number of requests to the same level at which call requests could be made from a telephone. Whilst the access limit is in place, if a user is not verified, the control levels will move through a second hack detection level, a third software download level and a fourth level where access is completely blocked for the apparatus 22.

20

The data processing apparatus 22 does not provide any unique identification (ID) when making an access request to the system 4 which can be used by the access control system 2, because an IP address is not unique for a machine 22 which is sharing a proxy server with other machines. The method therefore involves creating an ID which is
25 stamped on the requesting machine 22. Supplementary information delivery strategies currently supported by web browsers are cookie files and Secured Sockets Layer (SSL) client certificates, but as the availability of client certificates cannot be relied upon, the method uses encrypted cookie files, as described below. The A party user or the telephone 16 of the requesting A party is verified by executing an IVR based security check. The
30 access control server 6 instructs the IVR 8 to place a call to the telephone 16 designated in the call request, and the answering party is asked to enter or divulge a unique code which

- 5 -

back to the server 6 the code provided using the telephone 16. If the sent and received security codes correspond the A party is verified. A rate limit is therefore applied to a request having an IP address identifying the machine 22 until this IVR verification has been successfully completed.

5

The control levels of the access control method described below apply to unverified A party numbers from a given IP address. If m or more IP addresses in a segment are operating under a control level (m being an integer greater than or equal to 2), an entire IP segment, i.e. 256 addresses, is tagged as being in a control level. This provides protection from a hacker who is cycling through IP addresses in a segment. However, it is not until the fourth control level is reached that any IP address or segment blocking occurs, as this is potentially serious given that an entire proxy server can be blocked.

The first control level rate limits access requests so that the service is not denied to legitimate users and the telephone network is not adversely affected. At this level, the access method executes the IVR based verification or validation check, which additionally ensures that a computer 22 has been configured correctly.

When an initial access request is made by the data processing apparatus 22, the access control system 6 treats this initial access request as a request to register with the system 4 and enters a registration validation procedure where a time-limited encrypted cookie file encoded with a unique identification number is sent for storage at the machine 22 and can be used to make one call. When the A party is called for the first time, a random unique security code, which in this instance can be text based, is sent for display on the computer 22 and the IVR 8 is instructed by the access control system 6 to provide a prompt for the answering party at the telephone 16 to provide the displayed security code. If the security code is entered correctly by the answering party, using DTMF signals generated by pressing the buttons on the telephone 16, the time limit in the encrypted cookie is cancelled and the number of calls that can be made is changed to unlimited. The B party is then called on the telephone 18 or 20. Once the security code is verified the identification number in the cookie is sent with access requests to the application system 4.

- 6 -

The following rate limits are continuously imposed by the access control server 6 for unverified access requests:

1. One concurrent call per machine identification (ID), which is the preferred cookie ID rather than a SSL certificate ID.
- 5 2. One concurrent call per A party 16, identified by the A party number.
3. X concurrent calls per access system 2, which is the number of concurrent calls the system 2 is able to support.
4. One concurrent A party IVR validation procedure for a given IP address or segment.

10

Access requests or call requests that are received that exceed the above rate limits are queued by the access system 2 and a user is presented with their position in the queue on a page sent to the web browser of the user's machine 22. The queue position display also includes expected time in the queue. A configurable queue size limit applies to each
15 requesting IP address to prevent overuse of system resources.

The IVR validation check procedure is considered to have failed if an A party call is invalidated in that the call enters a ringing state and is abandoned or is connected and disconnected without the correct security code being entered into the telephone. This may
20 occur if a requesting party at the machine 22 enters an A party number which is not theirs and a telephone 18 or 20 is rung which is not associated with the machine 22. The person who receives this call of course cannot see the displayed security code on the screen of the machine 22. Essentially this will be a prank A party call.

25 The above procedures of the first security level, in particular the rate limit (no. 5) regarding concurrent registration and the time limit in the cookie, essentially eliminate any prank B party calls and limit the number of prank A party calls to about 2 to 6 per minute. The additional protection procedures in the additional control levels below limit the number of prank A party calls further so that only a few calls can be made.

- 7 -

The second access control level is entered if an IP address or segment fails a predetermined number, say n , IVR verifications or checks within the last 24 hours. The default for n would be 2. The purpose of this level is to execute additional tests on the user to ensure that a person is controlling the machine 22 and generating the access requests, as opposed to an automated program or hack. The tests in this level do not require the user to download any software to their computer 22.

The tests which are executed include the following:

1. A security code is again sent by the access control server 6 to the machine 22 for display and the IVR 8 instructed to call the A party telephone 16 and prompt for the security code to be entered. In this instance, however, the security code is presented in a graphic format, i.e. as a bitmap image. This will defeat any automated program which is simply looking for the code in a text based format, and will require any hacker to adjust the hacking program to incorporate optical character recognition which is sufficiently accurate to extract the security code.
2. Script or an applet is sent from the access control system to the machine 22 which is configured to scan the machine to detect an automatic continually iterative hacking program which may be making the access requests. This could be detected by a hacker.
3. The access control system 6 runs a check procedure to determine whether the HTTP requests from the machine 22 include data associated with normal use of most browsers, such as Netscape Navigator™ and Microsoft Internet Explorer™, and which would not normally be returned by a hacking program.
4. A time based test is executed also by the access control server 6 to detect whether the access requests are made faster than would be possible if the machine 22 was under human control.

Other remote checks for program control can also be executed.

- 8 -

This control level reduces the attack rate further by forcing a hacker to consider how to meet the above tests. This will take some time, believed to be at least 24 hours.

5 An IP address or segment at this control level will return to the first control level within 24 hours if no additional IVR verification failures occur. This will ensure that IP addresses randomly assigned by an Internet service provider (ISP) are not blocked simply because a hacker has generated a few prank calls.

10 The third access control level is entered if an IP address or segment fails n IVR tests, within 24 hours from the first access request, where n is greater than n .

15 In this control level, the access control server 6 sends a prompt to the user's machine 22 to download software to the machine 22. When a request for the software is received, the access control server 6 sends the software which, when stored on the machine 22, ensures all future communications between the machine 22 and the systems 2 and 4 is executed using a secure encrypted communications protocol. This prevents a hacker from determining the data passed between the machine 6 and the access control server 6 in all future communications. It also allows the downloaded software to examine the user's machine 22 and send investigative data securely back to the access control system 6 to
20 detect if a person or program is controlling the machine 22. Again, a hacker, after some time, may be able to break the encrypted communication protocol and create a wrapper program which mimics the downloaded software so that the hack can continue using the protocol to access the system 4. Again the time needed to break this control level is assumed to be at least 24 hours.

25

A machine 22 at the third control level returns to the first control level status within 48 hours from the initial access request if no additional IVR check failures occur. This is done, as mentioned previously, to allow release of IP addresses randomly assigned by ISPs.

30

An IP address or segment will reach the fourth control level and remain in this state until manually cleared by an operator of the system 2 if the IP address

- 9 -

failed $n+1$ IVR checks. This level is used to block the IP address or segment which is considered to be unverified. All access requests from the IP address or segment is refused. The block is made as close as possible to the machine 22, preferably at a router level, in the network 30 to reduce the performance impact of a continuous attack. Accordingly the
5 attack is reduced further by blocking the IP address or segment as close as possible to where the attack originates, which can block an entire proxy server.

The access control server 6 executes a reverse Domain Name Server (DNS) lookup procedure to determine the manager of the domain associated with the IP address or
10 segment and then sends an e-mail message to the manager advising the block has occurred. A copy of the e-mail is also sent to inform the operator of the systems 2 and 4.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the
15 accompanying drawing.

- 10 -

CLAIMS:

1. An access control method, including:
receiving an initial access request for a service from a data processing
5 apparatus;
sending unique identification data to said apparatus in response to said
initial access request; and
applying a rate limit for verifying access to said service until said
identification data is verified by a user of said apparatus.
10
2. An access control method as claimed in claim 1, wherein verifying said
identification data corresponds to a first level of access control, and said method
includes applying at least one additional level of access control following a
predetermined number of failed attempts to verify said identification data by said
15 user of said apparatus.
3. An access control method as claimed in claim 2, wherein said identification data is
a random unique security code and said apparatus is sent an unique identification
number which expires if the security code is not verified within a predetermined
20 period of time.
4. An access control method as claimed in claim 1, wherein said identification data is
verified by contacting a device with a known association to said user and said data
processing apparatus, and having said user provide said identification data using
25 said device.
5. An access control method as claimed in claim 1, wherein said identification data is
verified by said user returning said identification data using communication means
having a known association to said user and said data processing apparatus.

- 11 -

6. An access control method as claimed in claim 2, wherein said at least one additional level includes detecting generation of access requests for said service under control of a program instead of under control of said user.
- 5
7. An access control method as claimed in claim 2 or 6, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol.
- 10
8. An access control method as claimed in claim 7, wherein said communication software encrypts said access requests.
9. An access control method as claimed in claim 2, including invoking sequentially the levels of access control depending on the number of failed attempts to verify said identification data by said user for access requests over predetermined periods of time.
- 15
10. An access control method as claimed in claim 7 when dependent on claim 6, wherein said verifying of said identification data is a first level of access control, said detecting is a second level of access control, and said sending of said communication software and execution of said additional communication protocol is a third level of access control.
- 20
11. An access control method as claimed in claim 10, wherein said at least on additional level of access control includes a fourth level of access control involving blocking all access requests by said data processing apparatus.
- 25
12. An access control method as claimed in claim 11, wherein said blocking involves denying all access requests that include address data that corresponds to said data processing apparatus.
- 30

- 12 -

13. An access control method as claimed in claim 12, wherein the address data is an IP address or segment.
- 5 14. An access control method executed by a computer system, including:
applying an access rate limit until a user issuing access requests is verified;
a first control level involving verifying said user;
a second control level applying hack program detection tests to said access requests and verifying said user;
10 a third control level requiring use of predetermined download software for transmitting said access requests and verifying said user;
a fourth control level blocking access to said service on the basis of at least one communications address corresponding to said access requests; and
invoking said control levels sequentially depending on a number of failed
15 attempts to verify said user.
15. An access control method as claimed in claim 14, wherein said user is verified by contacting a device with a known association to said user and said data processing apparatus, and having said user provide identification data using said device.
20
16. An access control system having components for executing the steps of the access control method as claimed in any one of the preceding claims.
17. Access control software stored on a computer system, having code for executing
25 the steps of the access control method as claimed in any one of claims 1 to 15.
18. An access control system, including:
an access control server for receiving access requests for a service from a data processing apparatus, rate limiting access to the server until a user of said
30 apparatus is verified, and sending to said data processing apparatus unique identification data: and

- 13 -

an IVR for contacting a device having an association with said data processing apparatus, issuing a request for said identification data, and providing the data received in response to said request to said access server in order to verify said user.

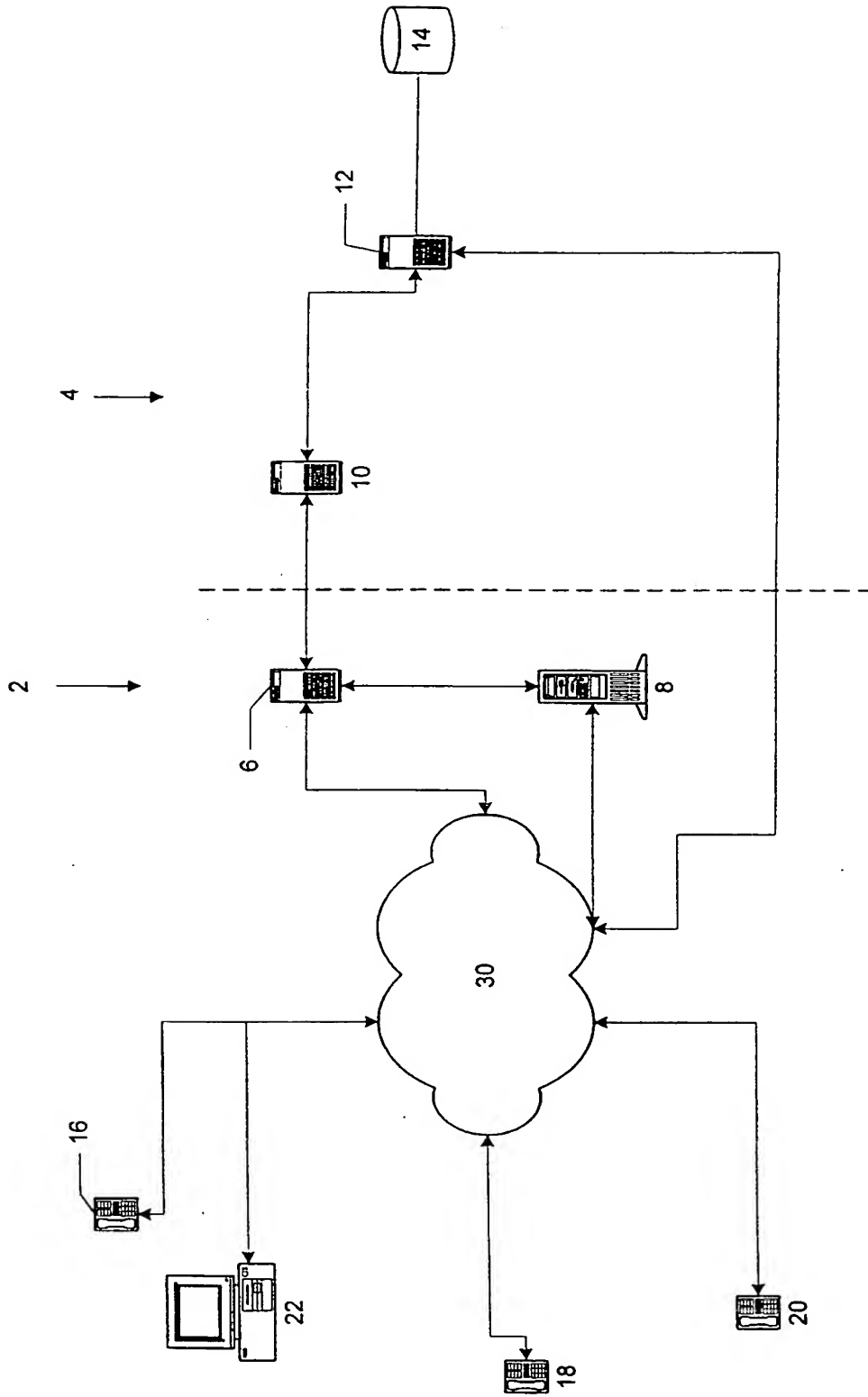


Figure 1

1553

DORSEY & WHITNEY LLP
4 EMBARCADERO CENTER SUITE 3400
SAN FRANCISCO, CA 94111-4187

2-3/710

DATE 8/20/2002

PAY TO THE ORDER OF COMMISSIONER OF PATENTS

\$ 40.00

FORTY DOLLARS

Security Features
Prevent Forgery
Check for Real

DOLLARS



Bank of America.

Commercial Disbursement Account • Chicago, Illinois

FOR 581 461124-00038

Robert B. Guckesing

MP

⑈001553⑈-⑈071000039⑈ 86660⑈17110⑈

RECORDATION FORM COVER SHEET

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

PATENTS ONLY

To the Honorable Assistant Commissioner for Patents and Trademarks. Please record the attached original documents or copy thereof.

<p>1. Name of conveying party(ies):</p> <p>Timothy Winston HIBBERD</p> <p>Additional name(s) of conveying party(ies) attached? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>	<p>2. Name and address of receiving party(ies):</p> <p>Name: <u>TELSTRA NEW WAVE PTY LTD</u></p> <p>Internal Address: _____</p> <p>Street Address: <u>242 Exhibition Street</u></p> <p>City: <u>Melbourne</u></p> <p>State: <u>Victoria</u> ZIP/Postal Code: <u>3000</u></p> <p>Country: <u>AUSTRALIA</u></p> <p>Additional name(s) & address(es) attached? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>3. Nature of Conveyance:</p> <p><input checked="" type="checkbox"/> Assignment <input type="checkbox"/> Merger</p> <p><input type="checkbox"/> Security Agreement <input type="checkbox"/> Change of Name</p> <p><input type="checkbox"/> Other _____</p> <p>Execution Date: <u>14 July 2002</u></p>	

4. Application number(s) or patent number(s):
If this document is being filed together with a new application, the execution date of the application is: _____

A. Patent Application No.(s)

10/088,034

B. Patent No.(s)

Additional numbers attached? ☐ Yes ☒ No

<p>5. Name and address of party to whom correspondence concerning document should be mailed:</p> <p>Name: <u>Michael A. KAUFMAN</u></p> <p>Internal Address: <u>DORSEY & WHITNEY LLP</u></p> <p>Street Address: <u>Four Embarcadero Center - Suite 3400</u></p> <p>City: <u>San Francisco</u></p> <p>State: <u>California</u> Zip: <u>94111-4187</u></p>	<p>6. Total number of applications and patents involved: 1</p> <p>7. Total fee (37 CFR § 3.41): \$ <u>40.00</u></p> <p><input checked="" type="checkbox"/> Enclosed</p> <p><input type="checkbox"/> Authorized to be charged to deposit account</p> <p>8. Deposit account number: <u>50-2319</u></p> <p>Please debit any underpayment or credit any overpayment to the above deposit account.</p> <p>Our Order No. <u>461124-00038 [A-71400]</u></p> <p>(Attach duplicate of this page if paying by deposit account)</p>
--	--

DO NOT USE THIS SPACE

9. Statement and signature.

To the best of my knowledge and belief, the foregoing information is true and correct and any attached copy is a true copy of the original document.

Michael A. KAUFMAN
Name of Person Signing

Michael A. Kaufman
Signature

20 August 2002
Date

Total number of pages including cover sheet, attachments and document: 2

OMB No. 0651-0011 (exp. 4/94)

Do not detach this portion

Mail documents to be recorded with required cover sheet information to:

Honorable Commissioner of Patents and Trademarks
Box Assignments
Washington, DC 20231

File No. A-71400/DJB/MAK

[461124-00038]
Rev. 8/93 (39811)
SF-1090722v1

ASSIGNMENT

WHEREAS, I/WE

Timothy Winston HIBBERD a Canadian citizen of 2/7 Bogota Avenue, Neutral Bay, New South Wales 2089, Australia;

hereinafter referred to as Assignor (collectively if more than one inventor is listed above), have invented certain new and useful improvements in (TITLE) **An access control method**

the specification of which:

- (a) ☐ was executed on even date herewith;
- (b) ☐ was filed on _____ as ☐ Application No. _____ or ☐ Express Mail No., as Application No. not yet known _____ and was amended on _____ (if applicable); or
- (c) ☒ was described and claimed in PCT International Application No. PCT/AU00/01095 filed on 13 September 2000 and as amended under PCT Article 19 on _____ (if any) and/or under PCT Article 34 on _____ (if any).

AND WHEREAS,

TELSTRA NEW WAVE PTY LTD, of 242 Exhibition Street, Melbourne, Victoria 3000, Australia

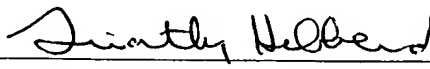
(hereinafter referred to as Assignee) desires to acquire the entire rights, title, and interest in and to the said improvements with respect to the United States of America, its territories and possessions.

NOW, THEREFOR, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Assignor hereby acknowledges that it has sold, assigned, transferred and set over, and by these presents does hereby sell, assign, transfer and set over, unto Assignee, its successors, legal representatives and assigns, the entire right, title, and interest in the United States of America, and its territories and possessions in, to and under said improvements, and any Patent Applications in the United States of America and all divisions, renewals and continuations thereof, and all Patents of the United States of America which may be granted thereon and all reissues and extensions thereof, and all rights of priority under International Conventions; and Assignor hereby authorizes and requests the Commissioner of Patents of the United States of America to issue all Patents for said improvements to Assignee, its successors, legal representatives and assigns, in accordance with the terms of this instrument.

AND ASSIGNOR HEREBY covenants and agrees that it will communicate to Assignee, its successors, legal representatives and assigns, any facts known to it respecting said improvements, and testify in any legal proceeding, sign all lawful papers, execute all divisional, continuing and reissue applications, make all rightful oaths and generally do everything possible to aid Assignee, its successors, legal representatives and assigns, to obtain and enforce proper patent protection for said improvements in the United States of America.

IN TESTIMONY WHEREOF, Assignor intending to be legally bound has hereunto affixed its signature.

This Fourteenth day of July, 2002


Timothy Winston HIBBERD

Witness



POWER OF ATTORNEY BY ASSIGNEE
(Not Accompanying Application)

The undersigned assignee of the entire interest in application for letters patent entitled: _____

An access control method

_____ and having the named inventors Timothy Winston HIBBERD September, 2000
_____, Serial No. PCT/AUS/01095, filed on or about the 13 day of July, 2000, hereby appoints the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith; said appointment to be to the exclusion of the inventor(s) and his (their) attorney(s) in accordance with the provisions of 37 C.F.R. 1.32:

Harold C. Hohbach, Reg. No. 17,757; Aldo J. Test, Reg. No. 18,048; Donald N. MacIntosh, Reg. No. 20,316; Edward S. Wright, Reg. No. 24,903; David J. Brezner, Reg. No. 24,774; Robert B. Chickering, Reg. No. 24,286; Richard F. Trecartin, Reg. No. 31,801; Steven F. Caserza, Reg. No. 29,780; Edward N. Bachand, Reg. No. 37,085; R. Michael Ananian, Reg. No. 35,050; Robin M. Silva, Reg. No. 38,304; Michael A. Kaufman, Reg. No. 32,988; Maria S. Swiatek, Reg. No. 37,244; Todd A. Lorenz, Reg. No. 39,754; Karen S. Smith, Reg. No. 31,426; Robert H. Pinsker, Reg. No. 42,078; Steven M. Freeland, Reg. No. 42,555; Larry Mendenhall, Reg. No. 38,555; Diane J. Mason, Reg. No. 43,777; William E. Nuttle, Reg. No. 42,943; James J. Diehl, Reg. No. 47,527; Renée M. Kossak, Reg. No. 47,717; Brian T. Clarke, Reg. No. 45,552; Anne M. Shyjan, Reg. No. 47,086; David C. Foster, Reg. No. 44,685; and Victor E. Johnson, Reg. No. 41,546; provided that if any one of said attorneys ceases being affiliated with the law firm of FLEHR HOHBACH TEST ALBRITTON & HERBERT LLP as partner, employee or of counsel, such attorney's appointment as attorney and all powers derived therefrom shall terminate on the date such attorney ceases being so affiliated.

In accordance with 37 CFR 3.73 the assignee hereby certifies that the evidentiary documents with respect to its ownership have been reviewed and that, to the best of assignee's knowledge and belief, title is in the assignee seeking to take this action.

Direct all telephone calls to _____ at (415) 781-1989.


Address all correspondence to:

FLEHR HOHBACH TEST ALBRITTON & HERBERT LLP
Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187

TELSTRA NEW WAVE PTY LTD

Assignee: _____

By: CHRIS ROWLES
(typed name)

Signature: 

Title: GM, TELSTRA NEW WAVE PTY LTD

Address: _____

File No. _____